

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-345664

(43)Date of publication of application : 05.12.2003

(51)Int.Cl.

G06F 12/14

G06F 1/00

H04L 9/14

(21)Application number : 2002-156931

(71)Applicant : NISSAN MOTOR CO LTD

(22)Date of filing : 30.05.2002

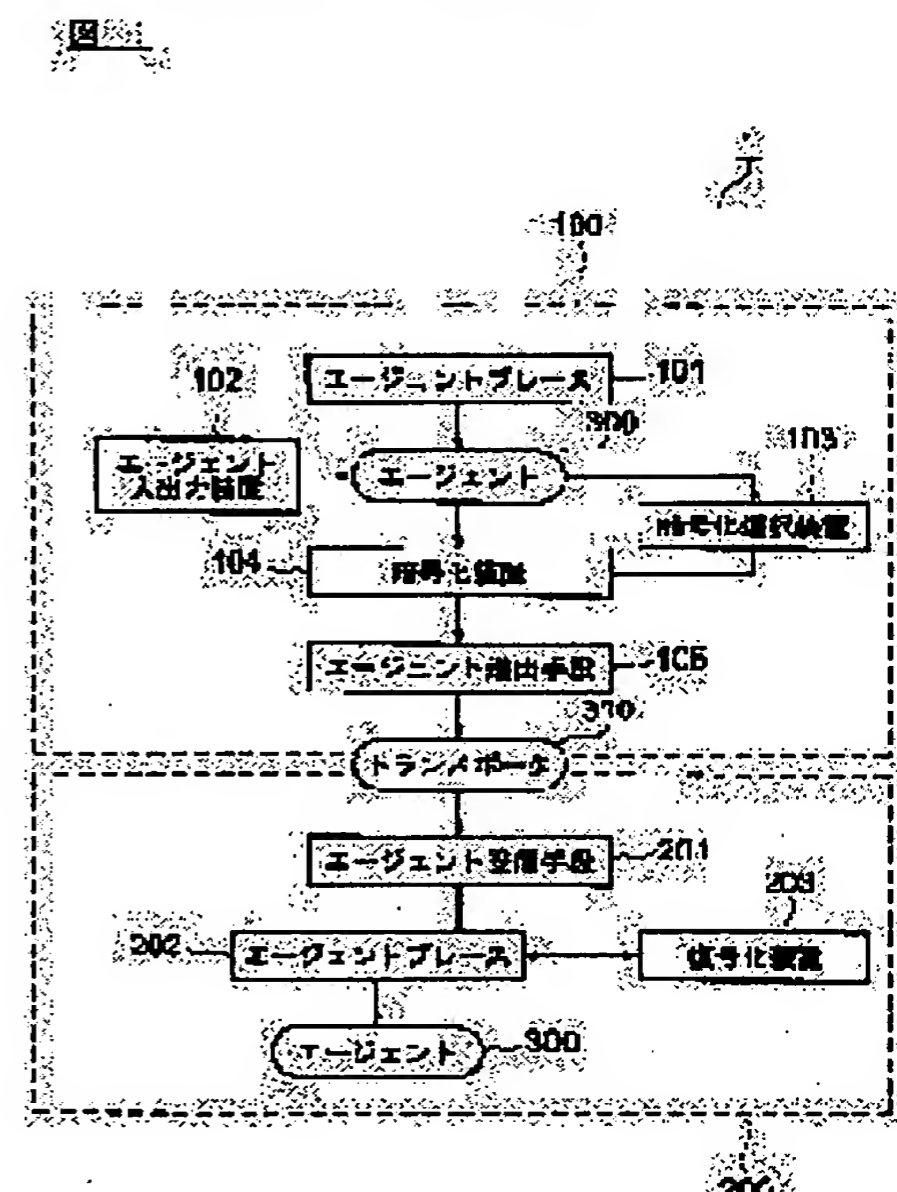
(72)Inventor : UEDA TETSUO

## (54) TRANSMISSION DEVICE, DATA PROCESSING SYSTEM, AND DATA PROCESSING PROGRAM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To prepare an autonomous program which manages security by itself by performing ciphering with optimum efficiency placing a small load on a computer resource while holding ciphering strength.

**SOLUTION:** In a transmission-side system 100, an agent place 101 generates an agent 300 having a program and data and sets a term of validity thereto. Further, a ciphering selecting device 103 selects a ciphering method which is strong enough not to allow illegal deciphering within the term of validity and a ciphering device 104 ciphers the agent. The this is sent from an agent sending-out means 105 to a reception-side system 200. After the term of validity expires, the agent disappears by itself. Therefore, data are ciphered within the term of validity, so illegal deciphering is no allowed and after the term of validity expires, the data are deleted, so that access is disabled even when deciphering is performed. The security of the data is properly ensured by the proper ciphering in which processing efficiency is taken into consideration.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (115PT0)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2003-345664  
(P2003-345664A)

(43) 公開日 平成15年12月5日 (2003.12.5)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
			3 2 0 B 5 B 0 7 6
			3 2 0 D 5 J 1 0 4
1/00		9/06	6 6 0 L
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1
審査請求 未請求 請求項の数19 O L (全 13 頁)			

(21) 出願番号 特願2002-156931(P2002-156931)

(22) 出願日 平成14年5月30日 (2002.5.30)

(71) 出願人 000003997

日産自動車株式会社

神奈川県横浜市神奈川区宝町2番地

(72) 発明者 上田 哲郎

神奈川県横浜市神奈川区宝町2番地 日産  
自動車株式会社内

(74) 代理人 100099900

弁理士 西出 眞吾 (外2名)

Fターム(参考) 5B017 AA06 AA07 BA08 BB09 BB10

CA15 CA16

5B076 FA01 FB18

5J104 AA12 AA16 AA36

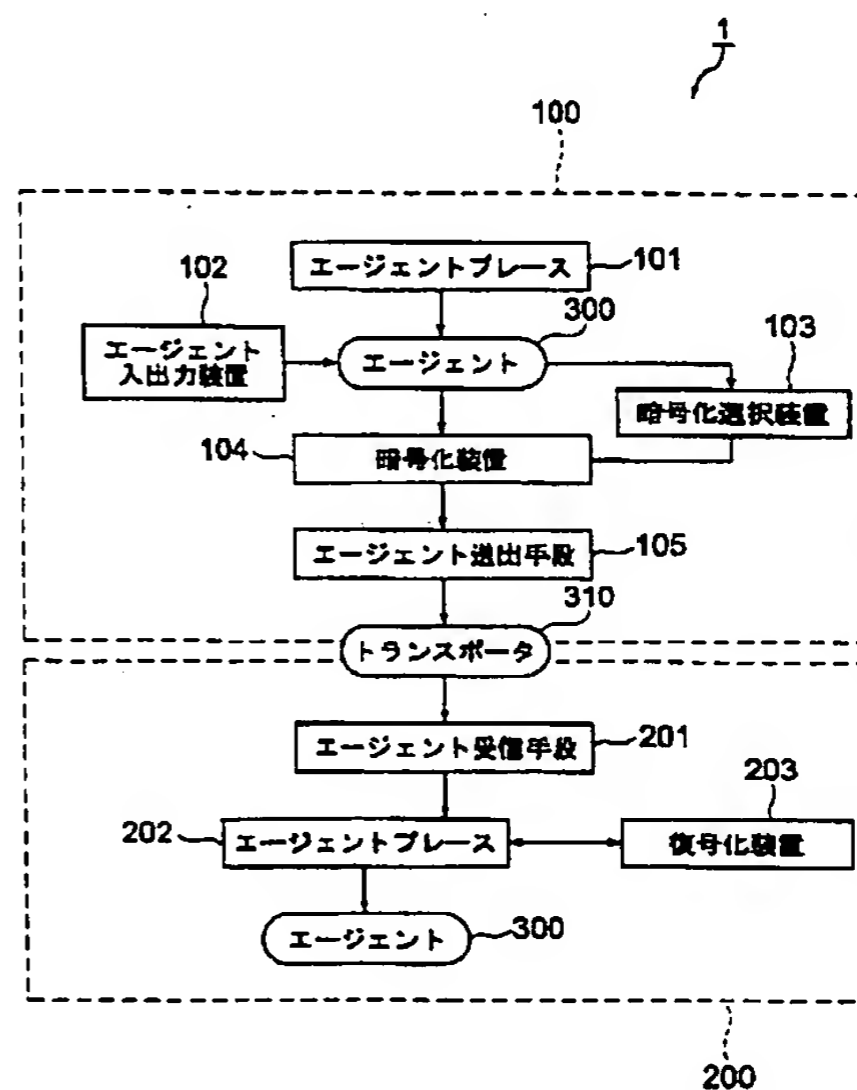
(54) 【発明の名称】 送信装置、データ処理システム及びデータ処理プログラム

(57) 【要約】

【課題】 暗号化強度を保ちつつ計算機リソースへの負荷が少ない効率が最適な暗号化を行い自ラセキュリティを管理する自律型プログラムを生成する。

【解決手段】 送信側システム100においては、エージェントブレース101がプログラム及びデータを有するエージェント300を生成し、これに有効期限を設定する。また、暗号化選択装置103で有効期限内に不正に復号化されない程度の強度の暗号化方法を選択し、暗号化装置104でエージェントを暗号する。そして、これをエージェント送出手段105より受信側システム200に送信する。なお有効期限が満了したらエージェントは自ら消滅する。従って、有効期限内はデータは暗号化されているので不正な復号化は許されず、有効期限満了後はデータが消滅しているため復号化されてもアクセスできない。従って、処理効率も考慮した適度な暗号化によりデータのセキュリティ性が適切に確保される。

図 1



## 【特許請求の範囲】

【請求項1】 計算機装置間を移動して実行されるプログラム及び任意のデータを有するオブジェクトを生成するオブジェクト生成手段と、

前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、

前記設定された有効期限内に不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、

前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、

前記データの暗号化されたオブジェクトを他の前記計算機装置に送信する送信手段とを有する送信装置。

【請求項2】 前記オブジェクトは、前記有効期限が満了した場合に自律的に消滅する請求項1に記載の送信装置。

【請求項3】 前記オブジェクトが有する前記プログラムは、前記有効期限が満了した場合に当該オブジェクトを自律的に消滅させるための記述を含む請求項2に記載の送信装置。

【請求項4】 前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含む請求項1～3のいずれかに記載の送信装置。

【請求項5】 前記オブジェクトを自律的に操作するための記述は、他の計算機装置に移動するためのオブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の、少なくともいずれか1つを含む請求項4に記載の送信装置。

【請求項6】 前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、かつできるだけ暗号化処理が容易な暗号化方法を選択する請求項1～5のいずれかに記載の送信装置。

【請求項7】 前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、

前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記データを暗号化する請求項1～6のいずれかに記載の送信装置。

【請求項8】 前記暗号化方法選択手段は、鍵の長さを選択し、

前記暗号化手段は、前記選択された長さの鍵を用いて前記データを暗号化する請求項1～7のいずれかに記載の送信装置。

【請求項9】 複数の計算機装置がネットワークを介して接続されたデータ処理システムであって、

計算機装置上で実行されるプログラム及び任意のデータを有するオブジェクトを生成するオブジェクト生成手段

と、

前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、

前記設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、

前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、

前記データの暗号化されたオブジェクトを送信する送信手段とを有する第1のデータ処理装置と、

前記送信されたオブジェクトを受信する受信手段と、

前記受信したオブジェクトに設定されている前記有効期限内である場合に、前記暗号化されたデータを復号化し、前記オブジェクトが有するプログラムを実行するプログラム実行手段と、

前記受信したオブジェクトに設定されている前記有効期限が満了した場合に、前記オブジェクトを消滅させるオブジェクト消滅手段とを有する第2のデータ処理装置とを有するデータ処理システム。

20 【請求項10】 前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、できるだけ暗号化処理が容易な暗号化方法を選択する請求項9に記載のデータ処理システム。

【請求項11】 前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、

前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記送信対象のデータを暗号化する請求項9又は10に記載のデータ処理システム。

30 【請求項12】 前記暗号化方法選択手段は、鍵の長さを選択し、

前記暗号化手段は、前記選択された長さの鍵を用いて前記送信対象のデータを暗号化する請求項9～11のいずれかに記載のデータ処理システム。

【請求項13】 前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び当該オブジェクトを自律的に操作するための記述を含み、

前記オブジェクト消滅手段においては、前記オブジェクトの前記プログラムが実行されることにより、当該オブジェクトの有効期限が満了した場合に該オブジェクトが消滅される請求項9～12のいずれかに記載のデータ処理システム。

【請求項14】 前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述、及び、前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含み、

前記プログラム実行手段においては、前記オブジェクトの前記プログラムが実行されることにより、前記所望の処理が終了した後に前記オブジェクトが自律的に操作される請求項9～13のいずれかに記載のデータ処

理システム。

【請求項15】前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述は、さらに他の計算機装置に移動するために当該オブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の少なくともいずれか1つを含む請求項14に記載のデータ処理システム。

【請求項16】コンピュータ上において所望の処理を実行するプログラム及び任意のデータを有するオブジェクト10  
であるデータ処理プログラムであって、  
前記コンピュータ上で前記データを参照して所望の処理を行う第1の機能と、予め設定された有効期限が満了したか否かを検出する第2の機能と、  
前記有効期限が満了した場合に、当該オブジェクトを消滅させる第3の機能とをコンピュータに実現させるデータ処理プログラム。

【請求項17】前記設定された前記オブジェクトの有効期限内に不正な方法により復号化されることが無い適切な強度の暗号化方法により、前記データが暗号化されている請求項16に記載のデータ処理プログラム。20

【請求項18】前記第1の機能による前記所望の処理の終了後に、前記オブジェクトを自律的に操作する第4の機能をさらにコンピュータに実現させる請求項16又は17に記載のデータ処理プログラム。

【請求項19】前記第4の機能は、他の計算機装置にさらに移動するために前記オブジェクトを複製する、前記オブジェクトを消滅する、及び、当該オブジェクトの生成元に帰着するの、少なくともいずれか1つの機能を実現する請求項18に記載のデータ処理プログラム。30

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、モバイルエージェントと言われる自律型のプログラムオブジェクトを用いて複数の計算機装置が接続されたネットワーク上において所望の処理を行うデータ処理システム、そのモバイルエージェントを生成してネットワーク上に送出する送信装置、及び、そのモバイルエージェントに含まれて実際にコンピュータ上においてそれらの処理を実現するデータ処理プログラムに関する。

【0002】

【従来の技術】一般的に、ソフトウェアプログラムは、スタンドアローン型及びクライアントサーバ型に大別される。スタンドアローン型は、計算機固有に記述されたネイティブなプログラムを直接ターゲットマシンにインストールして用いる方法である。一方、クライアントサーバ型は、クライアントマシン（ターゲットマシン）に搭載されたクライアントソフトウェアと、サーバに搭載されたサーバソフトウェアが協調して処理を行う方法であり、インターネットが普及した現在では、主にウェブ

ベースアプリケーションのことを指している場合が多い。ウェブベースアプリケーションは、実際にユーザが用いるプログラムはサーバ側にあり、ユーザはターゲットマシンに汎用的なWWWブラウザをインストールし、これよりネットワークを介してサーバ側プログラムを用いる方法である。

【0003】スタンドアローン型のメリットは、一般にプログラムがターゲットマシン固有に記述されているため処理が高速であるという点が挙げられる。また、ネットワークの利用が最低限で済むため、スピードの遅いネットワーク環境等においても、クライアントサーバ型のようにこのネットワークの遅さがボトルネックにならず、高速な処理が可能であるという点も挙げられる。

【0004】一方、スタンドアローン型のデメリットは、ユーザが、利用する全てのターゲットマシンに1つ1つソフトウェアプログラムをインストールしなければならないという点が挙げられる。ソフトウェアは、バージョンアップが宿命と言えるが、その度に、バージョンアップの手続き及びインストール処理を行わなければならない、大きな問題と言える。また、スタンドアローンシステムにおいては、一般に、ソフトウェアベンダー側がパッケージ化して用意したソフトウェア群をインストールして利用する場合が多いが、ユーザは必ずしもその全ての機能を必要としているわけではない場合がある。しかしながら、そのような場合も、ユーザは不必要な機能をも含む全てのソフトウェアプログラムをインストールせざるを得ず、必要な機能だけを必要な時にだけ利用するといった利用形態を実現することが難しい。その結果、計算機のリソースを圧迫することとなり、特に、モバイル端末のような記憶容量が限られており計算機リソースの浪費を抑えたいという環境下では問題である。

【0005】また、クライアントサーバ型のメリットは、ユーザはWWWブラウザさえ用意すればよく特別なソフトウェアのインストールの必要が無いという点が挙げられる。クライアントサーバ型は、WWWブラウザを用いて、必要な時に必要な機能のみをネットワークを介してサーバ装置より呼び出し利用するという形態であるため、利用するアプリケーションのバージョンは常に最新のものであるし、利用しない時にはソフトウェアプログラムは計算機中に存在せず、計算機リソースを浪費することが無い。なお、このようなクライアントサーバ型のメリットから、ASP（Application Service Provider）と呼ばれるアプリケーションプログラムの時間貸し業が注目されている。

【0006】クライアントサーバ型のデメリットは、ネットワークのボトルネックである。クライアントサーバ型では、表示や操作がクライアント側にあり、実際の処理はサーバ側で行うため、クライアントとサーバの間で頻繁にデータのやり取りが必要となり、データの授受を受け持つネットワークの性能がボトルネックとなる。例

えば、スタンドアローン型のシステムでは一瞬でできる処理も、クライアントサーバ型ではネットワークの遅延の影響を受け、待機時間が必要となる。一般に、ネットワークのスピードはメモリアクセス等のバススピードやCPUの処理スピードよりも遥かに遅いので、ネットワークの転送スピードがボトルネックになるのである。また、クライアントサーバ型のデメリットとして、一般にWWWブラウザのグラフィカルな表現力、インタフェースが限られたものであり、スタンドアローン型の多彩な表現やインタフェースに及ばないという問題もある。

【0007】ところで、このようなクライアントサーバ型とスタンドアローン型の間道的なアプローチで両方のメリットを享受しようとする試みに、Javaアプレットのようなプログラム逐次ダウンロード型のアプリケーションがある。近年広く使用されているいわゆるiモード携帯電話の1アプリケーションも、この種のアプリケーションの1つである。これは、ユーザはクライアントサーバ型の場合と同じくWWWブラウザのみをマシン内に備えるが、サーバ側にあるプログラムをその状態で使用するのではなく、WWWブラウザに一時的にダウンロードして用いるものである。これによって、従来のクライアントサーバ型では、ユーザの操作に応じて頻りにクライアントとサーバとの間でデータ交換が必要であったものが、プログラムがクライアント側に移動していることにより、データ交換が不要となり、クライアントサーバ型で問題となっていたネットワークボトルネックの問題を解消できるのである。

【0008】このタイプのプログラムは、最初のダウンロードにのみ時間がかかるが、その後は保存しておくこともできるので、まさにスタンドアローン型とクライアントサーバ型のメリットのみを持っていると言える。また、グラフィカルユーザインタフェースにおいても、Javaアプレットの場合では、同じWWWブラウザを用いながらスタンドアローン型とほぼ同程度の高度なインタフェースを実現できている。実際には、Javaアプレットにはセキュリティや互換性（インターオペラビリティ）に問題があるが、分散型のアプリケーションの向かうべき方向性を示していると言える。

【0009】このようなソフトウェアプログラムの実現形態の延長上にあるものとして、いわゆるモバイルエージェント型プログラムが挙げられる。このモバイルエージェント型プログラムについて、Javaアプレットのようなダウンロード型のプログラムと比較して説明する。ダウンロード型プログラムは、ユーザの要請によってサーバ側からダウンロードされ、ユーザが利用している間、ダウンロードされた計算機中に滞在して処理を行い、ユーザの利用が終わると終了して消滅するプログラムである。これに対して、モバイルエージェント型プログラムは、同じく計算機から計算機にプログラム本体がダウンロードされ、利用されるが、モバイルエージェン

ト自体が自律的に計算機の間を形を変えて移動したり、自身のクローンを作ったりして、それらの協調によりユーザの要求を処理するものである。端的な例で言えば、ダウンロード型プログラムがユーザの指示でダウンロードされるのに対して、モバイルエージェント型プログラムは、ユーザの指示によってユーザの要求をもってネットワークに出て行き、複数の計算機上でユーザの指示を実行して、戻ってくる（応えを持ち帰る）プログラムである。

10 【0010】

【発明が解決しようとする課題】ところで、このようなモバイルエージェント型プログラムは、ユーザの個人データのような機密データを持ち歩くケースも少なくない。例えば、モバイルエージェントが、個人の情報を持って航空機やホテルの予約のためにインターネットに出て行く場合等である。このような場合、従来のダウンロード型プログラムでは、サーバとクライアントの間のセキュアな通信さえ確保されていればデータのセキュリティ性が確保できていた。しかしながら、モバイルエージェント型プログラムでは、ユーザが送り出した後のエージェントの動作はもはやユーザからは制御できないため、管理できる範囲の通信のセキュリティ性を確保した程度では全体としてのセキュリティ性が確保されたとは言えないという事態となる。従って、モバイルエージェント型プログラムを用いたシステムにおいては、モバイルエージェント自らがデータ等のセキュリティ性を管理できるようにしたいという要望がある。

【0011】一方、データのセキュリティ性を確保するためには、データを暗号化することが考えられる。データの暗号化は、データの送り手と受け手が暗号鍵を共有化することによってデータを暗号化しデータの授受を排他的に行う仕組みであり、DES（Data Encryption Standard）のような共有鍵方式や、RSA（ronald Rivest, adi Shamir, lenard Adleman）等の秘密鍵方式が知られている。一般に、鍵の長さを例にとった場合、鍵長が長いほど暗号の強度が高まり安全であると言える。しかし、鍵長が長いほど、暗号化／復号化にも時間を要し、計算機リソースに相当の負荷を与えることとなる。この暗号化強度と計算機リソースの負荷の問題は、暗号化アルゴリズムの種類についても同様である。

【0012】モバイルエージェント型プログラムの場合には、汎用性や応答性等を維持するために、計算機リソースやネットワークリソースを無駄に浪費しないように考慮する必要がある。従って、このような暗号化を適用する場合においても、セキュリティ性を確保できるように暗号化の強度を保ちつつ、計算機リソースへの負荷がなるべく抑えられるような、すなわち効率が最適となるような暗号化を行いたいという要望がある。そして、そのために、モバイルエージェントが保護しようとしているデータに最適な暗号強度を選択したいという要望があ

る。

【0013】なお、保護すべきデータに応じて鍵やアルゴリズムを動的に変化させる方法としては、例えば特開平9-25899号公報に開示されている計算機中のCPUが処理するメモリ内部に蓄積されたデータを保護する手法がある。この手法によると、メモリ内のデータの暗号化／復号化を単調にいつも同じアルゴリズムや鍵を使っていたのでは、そのうちアルゴリズムや鍵が明らかになって暗号化の意味がなくなる心配があるので、データそのものの属性、つまり、メモリ上のアドレスや仮想記憶ページ番号等をキーにハッシュすることによって、暗号化／復号化の鍵やアルゴリズムを動的に変化させるというものである。しかしながらこの手法は、ランダムに鍵やアルゴリズムを選択することによって、暗号化／復号化の強度を高めようとするものであり、暗号化対象のデータに最適の鍵やアルゴリズムを動的に選択し、暗号化の強度を保ったままで最大の効率を確保するという目的を達成するものではない。

【0014】また、特開平11-282753号公報や、特開平10-340255号公報には、暗号そのものに有効期限を定めて期限を越えて復号化されないようにすることによって、セキュリティを高める方法が開示されている。しかし、この方法は、有効期限を設けることにより暗号化システムへの長期に渡る不正な復号処理の試行に歯止めをかけることを目的とするものであり、暗号化方法自体のセキュリティ性、計算機負荷の妥当性等について関わるものではなく、そのことについては何ら記載も示唆もされていない。

【0015】本発明はこのような問題点に鑑みてなされたものであって、本発明の目的は、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができるモバイルエージェントを送信する送信装置を提供することにある。また、本発明の他の目的は、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができるモバイルエージェントを用いて、ネットワーク上において効率よくセキュリティ性の確保された所望のデータ処理を行うことができるデータ処理システムを提供することにある。さらに、本発明の他の目的は、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができ、その状態でネットワーク環境上において所望の処理を実行するモバイルエージェントたるデータ処理プログラムを提供することにある。

【0016】

【課題を解決するための手段】前記目的を達成するために、本発明の第1の観点によれば、本発明の送信装置は、計算機装置間を移動して実行されるプログラム及び

任意のデータを有するオブジェクトを生成するオブジェクト生成手段と、前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、前記設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、前記データの暗号化されたオブジェクトを他の前記計算機装置に送信する送信手段とを有する（請求項1）。

10 【0017】このような構成の送信装置によれば、オブジェクト生成手段において計算機装置間を移動して実行されるプログラム及び任意のデータを有するオブジェクトを生成し、その生成されたオブジェクトに対して、有効期限設定手段において有効期限を設定する。そして、暗号化方法選択手段により、その設定された有効期限内に、不正な方法により復号化されることが無いような適切な強度の暗号化方法を選択し、暗号化手段においてその選択された暗号化方法により前記オブジェクトの前記データを暗号化している。そして、これら暗号化データを有し有効期限を設定されたオブジェクトを、所望の他の前記計算機装置に送信する。従って、オブジェクトが有効な期間はデータは暗号化されており不正な復号化を許さないもので、データのセキュリティが確実に確保される。また一方で、その有効期限後はデータが消滅されるので、暗号化によりセキュリティを確保する必要が無い。すなわち、有効期限満了後は、データ自身が消滅されているので、極端に言えば暗号化が不正に解読されることとなっても差し障りが無い。従って、暗号化方法選択手段における暗号化方法選択の際には、有効期限内のみ有効であるような適度の暗号化強度の暗号化方法を選択すればよく、結果的に過剰な暗号化強度を有し処理が複雑な暗号化方法を選択する必要がなくなる。

30 【0018】好適には、前記オブジェクトは、前記有効期限が満了した場合に自律的に消滅する（請求項2）。また好適には、前記オブジェクトが有する前記プログラムは、前記有効期限が満了した場合に当該オブジェクトを自律的に消滅させるための記述を含む（請求項3）。また好適には、前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含む（請求項4）。具体的かつ好適な例としては、前記オブジェクトを自律的に操作するための記述は、他の計算機装置にさらに移動するために当該オブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の、少なくともいずれか1つを含む（請求項5）。

40 【0019】また好適には、前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、かつ

できるだけ暗号化処理が容易な暗号化方法を選択する（請求項6）。また好適には、前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記データを暗号化する（請求項7）。また好適には、前記暗号化方法選択手段は、鍵の長さを選択し、前記暗号化手段は、前記選択された長さの鍵を用いて前記データを暗号化する（請求項8）。

【0020】また、本発明の第2の観点によれば、本発明のデータ処理システムは、複数の計算機装置がネットワークを介して接続されたデータ処理システムであって、計算機装置上で実行されるプログラム及び任意のデータを有するオブジェクトを生成するオブジェクト生成手段と、前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、前記設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、前記データの暗号化されたオブジェクトを送信する送信手段とを有する第1のデータ処理装置と、前記送信されたオブジェクトを受信する受信手段と、前記受信したオブジェクトに設定されている前記有効期限内である場合に、前記暗号化されたデータを復号化し、前記オブジェクトが有するプログラムを実行するプログラム実行手段と、前記受信したオブジェクトに設定されている前記有効期限が満了した場合に、前記オブジェクトを消滅させるオブジェクト消滅手段とを有する第2のデータ処理装置とを有する（請求項9）。

【0021】このような構成のデータ処理システムにおいては、第1のデータ処理装置のオブジェクト生成手段においてプログラム及び任意のデータを有するオブジェクトを生成し、その生成されたオブジェクトに対して有効期限設定手段において有効期限を設定する。また、その設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を暗号化方法選択手段において選択し、暗号化手段においてその選択された暗号化方法により前記オブジェクトのデータを暗号化する。そして、このプログラム及び暗号化データを有するオブジェクトが送信手段よりネットワークを解して所望の第2のデータ処理装置に送信される。第2のデータ処理装置においては、この送信されたオブジェクトを受信手段において受信し、設定されている有効期限の期間内である場合に、プログラム実行手段により暗号化されたデータを復号化してプログラムを実行する。また、有効期限が満了した場合には、オブジェクト消滅手段が前記オブジェクトを消滅させる。従って、オブジェクトが有効な期間はデータは暗号化されており不正な復号化を許さないの、データのセキュリティが確実に確保される。また一方で、その有効期限後はデータが消滅される

ので、暗号化によりセキュリティを確保する必要が無い。すなわち、有効期限満了後は、極端に言えば暗号化が不正に解読されることとなっても差し障りが無い。データ自身が消滅されているからである。従って、暗号化方法選択手段における暗号化方法選択の際には、有効期限内のみ有効であるような適度の暗号化強度の暗号化方法を選択すればよく、結果的に過剰な暗号化強度を有し処理が複雑な暗号化方法を選択する必要がなくなる。

【0022】好適には、前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、できるだけ暗号化処理が容易な暗号化方法を選択する（請求項10）。また好適には、前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記送信対象のデータを暗号化する（請求項11）。また好適には、前記暗号化方法選択手段は、鍵の長さを選択し、前記暗号化手段は、前記選択された長さの鍵を用いて前記送信対象のデータを暗号化する（請求項12）。また好適には、前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び当該オブジェクトを自律的に操作するための記述を含み、前記オブジェクト消滅手段においては、前記オブジェクトの前記プログラムが実行されることにより、当該オブジェクトの有効期限が満了した場合に該オブジェクトが消滅される（請求項13）。

【0023】また好適には、前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述、及び、前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含み、前記プログラム実行手段においては、前記オブジェクトの前記プログラムが実行されることにより、前記所望の処理が終了した後に前記オブジェクトが自律的に操作される（請求項14）。具体的かつ好適な例としては、前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述は、さらに他の計算機装置に移動するために当該オブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の少なくともいずれか1つを含む（請求項15）。

【0024】また、本発明の第3の観点によれば、本発明にかかるデータ処理プログラムは、コンピュータ上において所望の処理を実行するプログラム及び任意のデータを有するオブジェクトであるデータ処理プログラムであって、前記コンピュータ上で前記データを参照して所望の処理を行う第1の機能と、予め設定された有効期限が満了したか否かを検出する第2の機能と、前記有効期限が満了した場合に、当該オブジェクトを消滅させる第3の機能とをコンピュータに実現させるデータ処理プログラムである（請求項16）。

【0025】このような構成のデータ処理プログラムは、コンピュータに読み込まれてこれにより動作されることにより、第1の機能により具備する記データを参照して所望の処理が行われる。一方で、第2の機能により、予め設定された有効期限が満了したか否かが検出され、有効期限が満了していた場合には、第3の機能によりオブジェクト自らが消滅される。従って、読み込まれたコンピュータや、その背景のネットワーク等の環境に左右されることなく、有効期限がくればこのデータ処理プログラムたるオブジェクト自身が消滅し、保持されるデータ自身も消滅することとなり、これにより1つのセキュリティ性が確保される。また、このような条件があるので、このオブジェクトに含まれるデータを例えば暗号化する際には、この満了期間のみ不正なアクセスに耐え得る暗号化強度の暗号化を行えば十分であり、結果的に過剰な暗号化強度を有し、それがために処理する計算機リソース等に過大な負荷を与えるような暗号化を行うことがなくなる。すなわち、読み込まれて実行される処理環境に対して、不必要な過大な負荷を与えることが無く、処理効率のよいプログラムとなる。

【0026】好適には、前記設定された前記オブジェクトの有効期限内に不正な方法により復号化されることが無い適切な強度の暗号化方法により、前記データが暗号化されている（請求項17）。また好適には、前記第1の機能による前記所望の処理の終了後に、前記オブジェクトを自律的に操作する第4の機能をさらに有する（請求項18）。具体的かつ好適な例としては、前記第4の機能は、他の計算機装置にさらに移動するために前記オブジェクトを複製する、前記オブジェクトを消滅する、及び、当該オブジェクトの生成元に帰着するの、少なくともいずれか1つの機能を実現する（請求項19）。

【0027】

【発明の効果】このような構成の請求項1～8に記載の発明によれば、オブジェクト自身に有効期限を設定し、その有効期限までの期間、不正なアクセスからデータを保護することができる暗号化方法で暗号化を行うようにしており、暗号化の強度を保ちつつ計算機リソースへの負荷を必要最小限に抑えることができる。従って、最適な暗号化方法を選択し、セキュリティ性を自らが管理することができるモバイルエージェントを送信する送信装置を提供することができる。これに加えて請求項2に記載の発明によれば、モバイルエージェントは有効期限、すなわち寿命を迎えると送信者から制御されなくとも自動的に消滅し、保持しているデータも失われるので、一定時間（寿命）経過後に不正アクセス、盗聴等が行われることがなくなり、セキュリティが確実に確保される。

【0028】また、請求項3に記載の発明によれば、オブジェクトの有効期限満了に伴う消滅は、オブジェクト自らが保持するプログラムの記述に基づいて行われるため、ネットワーク上の種々のプログラム実行環境にお

て実行されるオブジェクトにおいては、環境の影響を受けることなく確実にオブジェクトを消滅できることとなり、セキュリティが確実に確保される。また、請求項4に記載の発明によれば、所望の処理の処理結果を含むオブジェクト自身等の処遇を、オブジェクト自らが規定することができ、ネットワーク環境に依存せずオブジェクト自らが管理したセキュリティ確保が可能となる。そして請求項5に記載の発明によれば、所望の処理が終了した後に、他の計算機装置へのさらなるオブジェクトの移動、オブジェクトの消滅、オブジェクト生成元への帰着等のオブジェクトの操作を行うことができる。

【0029】また、請求項6に記載の発明によれば、少なくともオブジェクトの有効期限の間のみ不正な復号化が不可能であるような暗号化強度で暗号化を行えばよく、過剰な暗号化強度で暗号化を行い計算機リソースを浪費する等の事態を防ぐことができる。また、請求項7に記載の発明によれば、暗号化アルゴリズムを選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。また、請求項8に記載の発明によれば、鍵長を選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。

【0030】また、前述した請求項9～15に記載の発明によれば、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができるモバイルエージェントを用いて、ネットワーク上において効率よくセキュリティ性の確保された所望のデータ処理を行うことができるデータ処理システムを提供することができる。これに加えて請求項10に記載の発明によれば、少なくともオブジェクトの有効期限の間のみ不正な復号化が不可能であるような暗号化強度でなるべく処理が簡単な暗号化方法で暗号化を行えばよく、過剰な暗号化強度で暗号化を行い計算機リソースを浪費する等の事態を防ぐことができる。また、請求項11に記載の発明によれば、暗号化アルゴリズムを選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。また、請求項12に記載の発明によれば、鍵長を選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。

【0031】また、請求項13に記載の発明によれば、オブジェクトの有効期限満了に伴う消滅は、オブジェクト自らが保持するプログラムの記述に基づいて行われるため、ネットワーク上の種々のプログラム実行環境において実行されるオブジェクトにおいては、環境の影響を受けることなく確実にオブジェクトを消滅できることとなり、セキュリティが確実に確保される。また、請求項14に記載の発明によれば、所望の処理の処理結果を含むオブジェクト自身等の処遇を、オブジェクト自らが規定することができ、ネットワーク環境に依存せずオブジェクト自らが管理したセキュリティ確保が可能となる。

そして請求項15に記載の発明によれば、所望の処理が終了した後に、他の計算機装置へのさらなるオブジェクトの移動、オブジェクトの消滅、オブジェクト生成元への帰着等のオブジェクトの操作を行うことができる。

【0032】また、前述した請求項16～19に記載の発明によれば、セキュリティ性を自ら管理することができ、その状態でネットワーク環境上において所望の処理を実行するモバイルエージェントたるデータ処理プログラムを提供することができる。これに加えて請求項17に記載の発明によれば、少なくともオブジェクトの有効期限の間のみ不正な復号化が不可能であるような暗号化強度によりデータが暗号化されているので、過剰な暗号化強度で暗号化を行い計算機リソースを浪費する等の事態を防ぐことができる、効率よい処理を行うデータ処理プログラムを提供することができる。また、請求項18に記載の発明によれば、所望の処理の処理結果を含むオブジェクト自身等の処遇を、オブジェクト自らが規定することができる、ネットワーク環境に依存せずオブジェクト自らが管理したセキュリティ確保が可能となる。そして請求項19に記載の発明によれば、所望の処理が終了した後に、他の計算機装置へのさらなるオブジェクトの移動、オブジェクトの消滅、オブジェクト生成元への帰着等の自らの操作を行うことができる。

【0033】

【発明の実施の形態】本発明の一実施の形態について図1～図4を参照して説明する。本実施の形態においては、モバイルエージェントと言われるオブジェクトをネットワーク上に配置することにより、ネットワーク上で所望のデータ処理を行うデータ処理システムを例示し、特にそのモバイルエージェントの取り扱い方法を説明することにより本発明を説明する。

【0034】まず、そのデータ処理システムの構成について説明する。図1は、本実施の形態のデータ処理システム1の構成を示すブロック図である。図1に示すように、データ処理システム1は送信側システム100及び受信側システム200を有する。また、図示しないが、送信側システム100と受信側システム200とは、任意にデータ伝送可能にネットワークにより接続されている。このネットワークは、Java及びTCP/IPをベースとしたネットワークであり、本実施の形態においてはインターネットとする。

【0035】送信側システム100は、モバイルエージェントを生成しネットワークを介して受信側システム200に送信する例えばパーソナルコンピュータ等の計算機装置である。送信側システム100は、エージェントブレース101、エージェント入出力装置102、暗号化選択装置103、暗号化装置104及びエージェント送出手段105を有する。

【0036】エージェントブレース101は、モバイルエージェント300のオブジェクトを生成する。具体的

には、送信側システム100の計算機リソースのメモリ上に、モバイルエージェント300のオブジェクトを確保することにより、モバイルエージェント300の実体を生成し、さらにモバイルエージェント300とエージェントブレース101との間で相互に参照可能にポインタを張ることにより、モバイルエージェント300を登録する。そして、モバイルエージェント300に独自のスレッドを割り当てることにより、モバイルエージェント300を起動する。この時、エージェントブレース101は、モバイルエージェント300に、消滅するまでの有効期限（寿命）をセットする。なお、この寿命は、モバイルエージェントごとに個別の値がセットされる。

【0037】エージェント入出力装置102は、モバイルエージェント300に対する指示等を入力する。モバイルエージェント300に特段の指示等がある場合には、エージェントブレース101におけるモバイルエージェント300の生成後に送信側システム100は入力フェーズに入る。その結果、エージェント入出力装置102に適宜必要なダイアログボックス等が表示されて、所望の指示が入力される。

【0038】暗号化選択装置103は、モバイルエージェント300が保持しているデータを暗号化するための暗号化条件を選択する。暗号化選択装置103は、モバイルエージェント300に設定されているモバイルエージェント300の寿命、及び、モバイルエージェント300のサイズに基づいて、暗号化強度が最適となるような暗号化条件を選択し、その条件でモバイルエージェント300が保持するデータの暗号化を行うよう、実質的に暗号化装置104に指示する。より具体的には、具備している暗号化アルゴリズムより最適な暗号化アルゴリズムを選択し、また、その暗号化アルゴリズムに対して最適な鍵長を検索し、その暗号化アルゴリズム及び鍵長を暗号化装置104に指定する。なお、暗号化選択装置103における暗号化条件の選択基準等については、後に詳細に説明する。

【0039】暗号化装置104は、暗号化選択装置103より指定された暗号化アルゴリズム及び鍵長により、モバイルエージェント300が保持するデータを暗号化する。なお、暗号化選択装置103における暗号化処理の具体的な手順については、後に詳細に説明する。

【0040】エージェント送出手段105は、暗号化装置104において暗号化された暗号化データを含む送信対象のモバイルエージェント300を、受信側システム200に送信する。具体的には、エージェント送出手段105は、暗号化データを含むモバイルエージェント300のデータをトランスポータ310の中に配置し、受信側システム200のエージェント受信手段201に対してJavaのvisitの因数として引き渡す。その結果、Javaは訪問先へのストリームを開き、トランスポータオブジェクトを直列化してストリームに入力す

る。なおこの時、エージェント送出手段105は、モバイルエージェント300のクラスの定義も受信側システム200に送信する。

【0041】受信側システム200は、送信側システム100より送信されるモバイルエージェント300を受信し、モバイルエージェント300に含まれる暗号化データを復号化して所望の処理を行う装置であって、送信側システム100と同じく例えばパーソナルコンピュータ等の計算機装置である。受信側システム200は、エージェント受信手段201、復号化装置203及びエ

ージェントブレース202を有する。  
【0042】エージェント受信手段201は、Javaの機能としてストリームからモバイルエージェント300を取り出し、モバイルエージェントオブジェクトの実体をエージェントブレース202上に復元する。また、送信側システム100からは、モバイルエージェント300とともにモバイルエージェント300のクラス定義データが転送されるので、エージェント受信手段201は、クラスローダによって新たなクラスをJava Virtualマシンに登録する。これにより、モバイルエ

ージェント300の新たなタイマが動作を始める。  
【0043】エージェントブレース202は、復元されたモバイルエージェント300に独自のスレッドを割り当てることにより、モバイルエージェント300を起動する。

【0044】復号化装置203は、復元されたモバイルエージェントに含まれる暗号化データを復号化し、復号化されたデータをモバイルエージェント300に供する。なお、復号化装置203における復号化処理の具体的な手順については、後に詳細に説明する。

【0045】保持するデータが復号化されたモバイルエージェント300は、1つの独立したオブジェクトとして、その内部に記述されているプログラムによって、そのモバイルエージェント300に固有の所望の処理を行う。その固有の処理が終了したら、次に、モバイルエージェント300は、その所望の処理の結果及びモバイルエージェント300自身を操作する処理を行う。この処理は、モバイルエージェント300の動作としてモバイルエージェント300中に記述してあるプログラムに従って実行される場合と、エージェントブレース202が独自に処理を選択し実行する場合とがある。しかしどちらの場合も、その処理としては、複製、消滅又は帰着のいずれかの処理が実行されることとなる。

【0046】複製は、モバイルエージェント300自身の複製(クローン)を生成し、そのクローンエージェントをさらなる別の訪問先へ、図示せぬ受信側システム200より訪問させる処理である。これは、例えば、最初に訪れたエージェントが単なるハブで他のエージェントブレースへのポインタに過ぎない場合等に、エージェントブレース202の判断により選択され実行される。つ

まり、訪れたエージェントブレースは、他のエージェントブレースへの案内場所であり、かつ、その案内場所が複数ある場合に、エージェントブレースはエージェントを次に訪れるエージェントブレースの場所の数だけ複製(クローン)し、それぞれのエージェントブレースに移動させる。なお、この複製処理が行われた場合、複製される前の元のモバイルエージェント300は、最終的に消滅する。従って、この時点でエージェントが保持していたデータへのアクセスは不可能になる。

【0047】消滅は、エージェントの寿命(最初に設定された有効期間)が訪れた場合に、自身のスレッドを停止し、エージェントブレース202からメモリを開放する処理である。メモリの実質的な開放は、Javaのガベージコレクションによって行われる。モバイルエージェント300は、送信側システム100の暗号化選択装置103によって最適な暗号化強度のアルゴリズム及び鍵長が選択されて暗号化が行われているので、寿命が訪れるまでにアタックされるどのような鍵無し復号化も、モバイルエージェント300の消滅までに復号化は行えない。

【0048】帰着は、最初の指示によってホームである送信側システム100に戻る処理である。これは、訪問先でモバイルエージェント300が得た処理結果を送信側システム100に持ち帰るような場合に相当する。その場合は、受信側システム200内の図示しないエージェント送出手段によってモバイルエージェント300は送信側システム100に送信され、送信側システム100の図示しないエージェント受信手段によりモバイルエージェント300は受信される。送信側システム100に戻ったモバイルエージェント300は、持ち帰った処理結果をエージェントブレース101に返した後、消滅の処理を行う。つまり、スレッドを停止し、ホームのJavaのガベージコレクターによりメモリを開放する。この時点でホームに戻ったエージェントが保持していたデータへのアクセスも不可能になる。

【0049】次に、このような構成のデータ処理システム1の送信側システム100の暗号化選択装置103及び暗号化装置104、及び、受信側システム200の復号化装置203における暗号化及び復号化の具体的処理について、図2及び図3を参照して説明する。

【0050】まず、送信側システム100の暗号化選択装置103における、暗号化強度の選択条件、選択方法について、図2を参照して説明する。図2は、暗号化されたモバイルエージェント300を復号鍵を知らずに復号化する時間と、モバイルエージェント300の寿命の関係を示す図である。時間Taを暗号化アルゴリズムAで暗号化されたデータを復号鍵aを用いて復号化するのに要する時間、時間Tbをその暗号化データを復号鍵を知らずに復号化するのに要する時間とすると、一般にTa < Tbの関係が成り立つ。そして、時間Tをモバイル

エージェントの寿命とすると、 $T_a < T < T_b$ の関係が成り立つ場合に、この暗号化アルゴリズム及び鍵の選択は適切である、すなわち暗号化システムとして成立すると言える。すなわち、正当な復号鍵 $a$ を保持する者は暗号化データを復号して平文データを獲得することができ、復号鍵を知らずに暗号化データの復号を試みた場合には、復号化を達成する前にモバイルエージェント自体が寿命により消滅してしまう状態である。

【0051】ところで、この条件は、復号鍵を知らずに復号化する時間 $T_b$ とモバイルエージェント300の寿命 $T$ との関係で示すと、図2の斜線領域で示す条件となり、この斜線領域に含まれる条件であれば、どのような条件であっても暗号化システムとしての目的、性能は達成されたものとなる。従って、暗号化システムの効率を考えた場合には、図2に領域321で示すような、復号鍵を知らずに復号化が行える時間 $T_b$ がモバイルエージェントの寿命 $T$ よりもやや長くなる程度の暗号化強度が好ましい、すなわち暗号化アルゴリズム及び鍵長が、安全にデータを送信するために必要かつ十分な最適な条件と言える。逆に言えば、図2に領域322で示すような、復号化鍵を知らずに復号するのに要する時間 $T_b$ がモバイルエージェントの寿命 $A$ よりも遥かに長いようなアルゴリズム又は鍵長は、復号化が達成される遥か前にモバイルエージェント自体が消滅しているため無意味であり、そのような暗号化を行うこと自体が計算機リソースを無駄使いしていると言える。

【0052】従って、送信側システム100の暗号化選択装置103においては、エージェントブレース101で設定されたモバイルエージェント300の寿命 $T$ に基づいて、復号鍵を知らずに復号化が行える時間 $T_b$ がモバイルエージェントの寿命 $T$ よりもやや長くなるような、図2に領域321で示すような最適な暗号化強度、すなわちアルゴリズム及び鍵長を動的に選択し、モバイルエージェント300に適用する。

【0053】次に、送信側システム100の暗号化装置104及び受信側システム200の復号化装置203における実際の暗号化及び復号化の手順について、図3を参照して説明する。インターネット等のネットワークを介して不特定多数との暗号通信のためには、通常、秘密鍵方式の暗号化手法を用いるが、本実施の形態のようにモバイルエージェント300を用いて秘密鍵方式の暗号化通信を行うには、基本的に以下のような手順で処理を行う。

- (1) 送信前に送信先のエージェントブレースの公開鍵を入手する。
- (2) 公開鍵でデータを暗号化する。
- (3) 送信先のエージェントブレースに移動する。
- (4) 送信先のエージェントブレースは秘密鍵でエージェントが保持するデータを復号化する。

【0054】以下、この手順による暗号化及び復号化の

具体的な手順について、図3に示すフローチャートを参照して説明する。まず、送信側システム100の暗号化装置104においては、暗号化対象のデータ401からMD5一方向ハッシュ関数402等によって、メッセージダイジェスト403を作成する(ステップS11)。次に、RSA秘密鍵404等によって、ステップS11で作成したメッセージダイジェスト403を暗号化する(ステップS12)。一方、乱数406を鍵として、DES等の共有鍵暗号化形式の共有鍵407を生成する(ステップS13)。

【0055】そして、ステップS13で生成した共有暗号鍵407によって、ステップS12で生成した暗号化メッセージダイジェスト405及びデータ401を暗号化し、暗号化データ408を生成する(ステップS14)。また、訪問先の公開鍵409によって、ステップS13で生成した共有鍵を暗号化し、暗号化された共有鍵410を生成する(ステップS15)。そして、ステップS14で生成した暗号化データ408及びステップS15で生成した暗号化共有鍵410を、受信側システム200に送信する(ステップS16)。

【0056】受信側システム200の復号化装置203においては、送信され暗号化データ408及び暗号化共有鍵410を受信し(ステップS16)、秘密鍵411によって送信されてきた暗号化共有鍵410を復号化して共有鍵407を取り出す(ステップS17)。そして、送られてきた暗号化データ408を、ステップS17で復号化した共有鍵407で復号化することにより、復号化された平文のデータ401が得られる(ステップS18)。

【0057】ステップS18の復号化の際には、暗号化メッセージダイジェスト405も同時に得られるので、これを、送信側システム100側の公開鍵413で復号化し、送信側システム100側で生成されたメッセージダイジェスト403を得る(ステップS19)。また、ステップS18で復号化したデータ401から、MD5一方向ハッシュ402によってメッセージダイジェスト414を作成する(ステップS20)。そして、ステップS19で復号化したメッセージダイジェスト403と、ステップS20で新たに作成したメッセージダイジェスト414を比較する(ステップS21)。その結果、これらのメッセージダイジェスト403、414が一致した場合は、送信側の認証と改竄がないことが証明され、データ401の授受が完了する。

【0058】最後に、このような構成のデータ処理システム1の動作について、モバイルエージェント300の動作として、図4を参照してまとめて説明する。まず、送信側システム100において、エージェントの親プログラムであるエージェントブレース101が、送信側システム100の計算機リソース上のメモリにエージェントの実体(オブジェクト)を確保することにより、モバ

イルエージェント300の実体が生成される(ステップS31)。このときに、エージェントブレース201は、モバイルエージェント300に、消滅するまでの有効期限(寿命)をセットする。生成されたモバイルエージェント300は、エージェントブレース101へ登録されることにより配置され(ステップS32)、モバイルエージェント300に固有のスレッドを起動することにより起動される(ステップS33)。

【0059】何らかの入力項目がある場合には、モバイルエージェント300はここで入力フェーズに入り、エージェント入出力装置102を介した入力操作を受け付ける(ステップS34)。次に、エージェントのサイズと寿命によって、暗号化選択装置103を介して最適な暗号化アルゴリズム及び鍵長を検索し、暗号化装置104によって保持するデータを暗号化する(ステップS35)。そして、エージェント送出手段105より、受信側システム200(訪問先)へ送信される(ステップS36)。

【0060】受信側システム200においては、エージェント受信手段208がJavaの機能としてストリームからエージェントを取り出し、エージェントオブジェクトの実体をエージェントブレース203上に復元し(ステップS37)、同時に転送されるエージェントのクラスをクラスローダJavaVirtualマシンに登録することにより、新たにエージェント203の寿命タイマが動作する。そして、モバイルエージェント300は、再び再び独自のスレッドを開始し起動する(ステップS38)。

【0061】起動されたら、モバイルエージェント300は、復号化装置203を介して暗号化データを復号化し(ステップS39)、復号化されたデータを用いてエージェント固有の処理を行う(ステップS40)。そして、エージェント固有の処理が終了したら、その処理結果及び自らのその後の処理として、モバイルエージェント300内部に記載されているプログラムに従って、又はエージェントブレース202からの制御に基づいて、複製(ステップS41)、消滅(ステップS42)、帰着(ステップS43)のいずれかの処理を実行する。

【0062】このように、本実施の形態のデータ処理システム1によれば、モバイルエージェント300が自律的に保持しているデータを管理する方法として、モバイルエージェント300自体に有効期限を設けるようにした。モバイルエージェントの送信者が、ネットワーク上にモバイルエージェント300を送出した後は、モバイルエージェント300が移動やクローン化を自律的行うために、送信者は、今現在どこに自分の送り出したモバイルエージェント300が存在しているかもわからないし、通信手段もわからないのが一般的である。しかし、モバイルエージェントに寿命を設定することによって、送信者から制御されなくとも、モバイルエージェン

トは生成されてから一定期間経つと、そのデータともども自動的に寿命を迎えて消滅する。そして、消滅すればデータも失われ、盗聴や不正アクセス等の危険はなくなる。従って、このような自律型のモバイルエージェント300を用いた自律型のプログラムオブジェクトを用いたデータ処理システムにおいても、適切なセキュリティが確保される。

【0063】なお、場合によっては、まだ使命を終えていないにも関わらず寿命を迎えてしまうモバイルエージェントも存在することになるが、モバイルエージェントをベースとしたアプリケーションは、場合によっては応えが帰らない場合もあるというベストエフォート型のサービスとして認識されることにより障害はなくなる。

【0064】なお、本実施の形態は、本発明の理解を容易にするために記載されたものであって本発明を何ら限定するものではない。本実施の形態に開示された各要素は、本発明の技術的範囲に属する全ての設計変更や均等物をも含み、また、任意好適な種々の改変が可能である。例えば、本実施の形態においては、自律型のプログラムオブジェクトとして、いわゆるモバイルエージェントを示したが、本発明においては、汎用的な計算機装置やノード装置等で構成される一般的なプラットフォーム、環境中において、装置に依存した特定の制御動作に依存することなく自律的に動作可能なオブジェクトであれば、任意のオブジェクトでよく、何ら本実施の形態のオブジェクトの具体的な構成、動作手順等に限定されるものではない。

【0065】また、本実施の形態においては、送信側システム100及び受信側システム200は、汎用的なネットワークに各々1つのノードとして配置されている装置であるとしたが、2台の例えばパーソナルコンピュータ等が直接に通信回線で接続されたような処理システムや、よりローカルな通信ネットワークにより接続された各端末装置等であってもよく、何らシステムセンタの構成が限定されるものではない。その他、暗号化及び復号化の方法等も任意の方法でよい。

#### 【図面の簡単な説明】

【図1】図1は、本発明の一実施の形態のデータ処理システムの構成を示すブロック図である。

【図2】図2は、暗号化されたモバイルエージェントを復号鍵を知らずに復号化する時間とモバイルエージェントの寿命の関係を示す図である。

【図3】図3は、図1に示したデータ処理システムにおける、送信側システムの暗号化装置及び受信側システムの復号化装置における暗号化及び復号化の手順を示すフローチャートである。

【図4】図4は、図1に示したデータ処理システムにおけるモバイルエージェントの動作を示すフローチャートである。

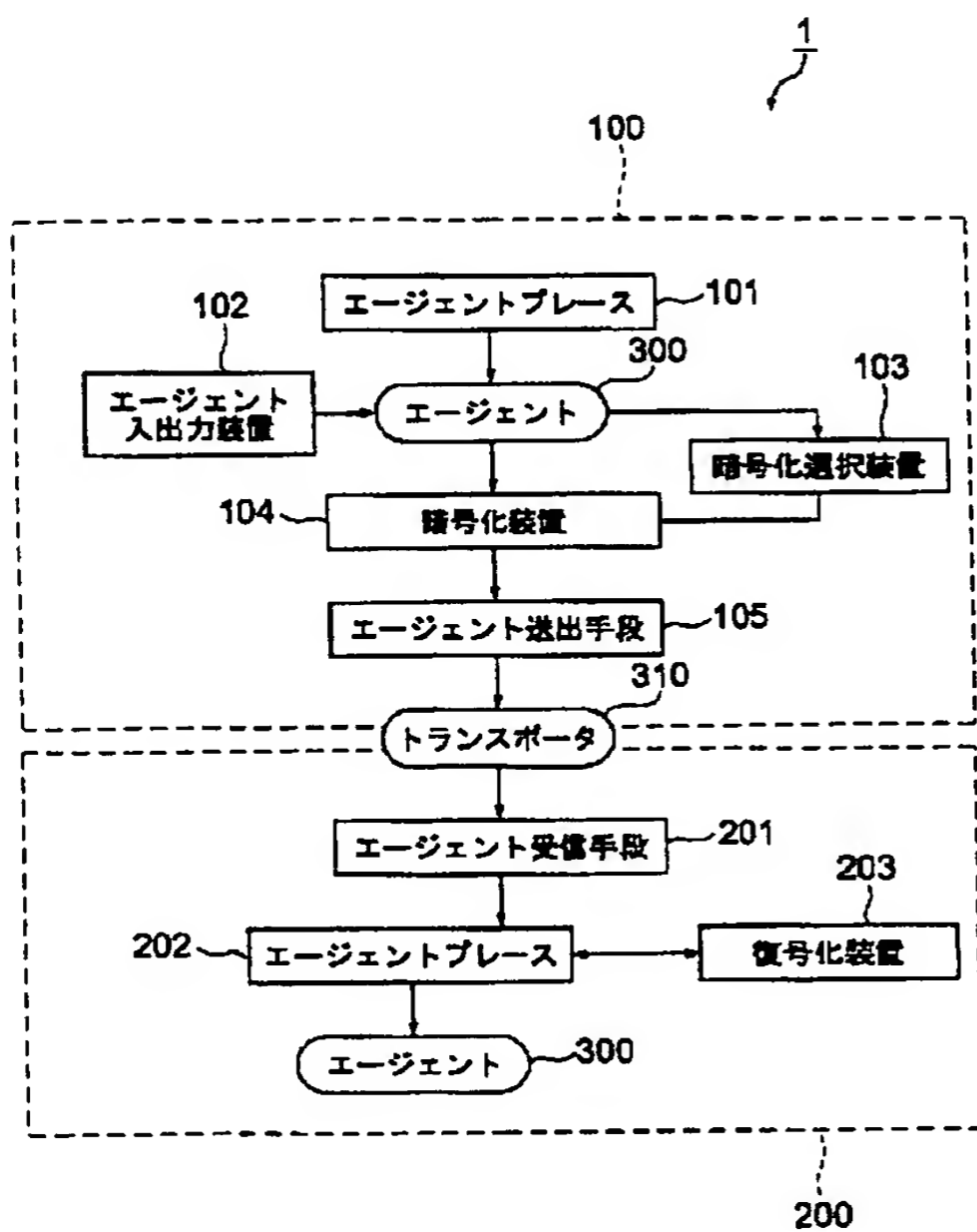
#### 【符号の説明】

21

100…送信側システム  
 101…エージェントブレース  
 102…エージェント入出力装置  
 103…暗号化選択装置  
 104…暗号化装置  
 105…エージェント送出手段  
 200…受信側システム  
 201…エージェント受信手段  
 202…エージェントブレース  
 203…復号化装置  
 300…モバイルエージェント  
 401…データ

【図1】

図 1

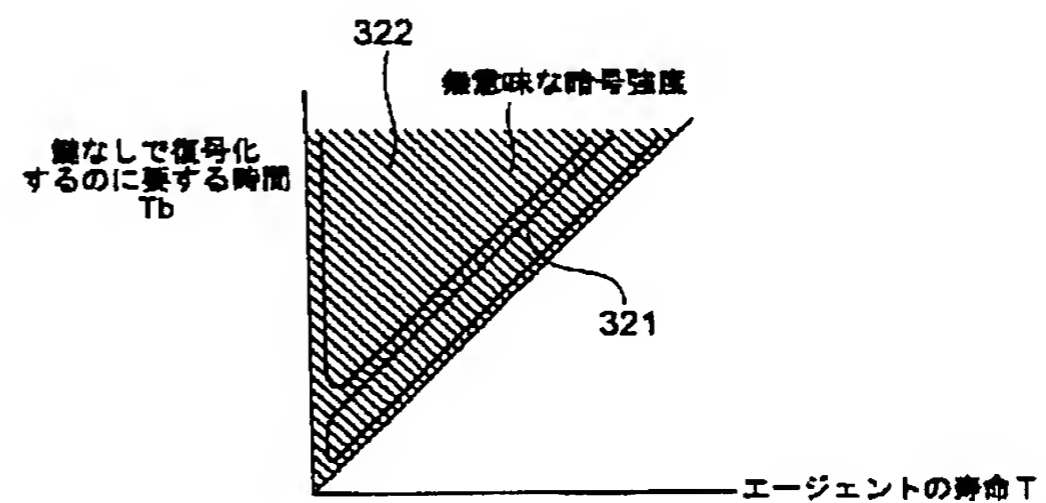


22

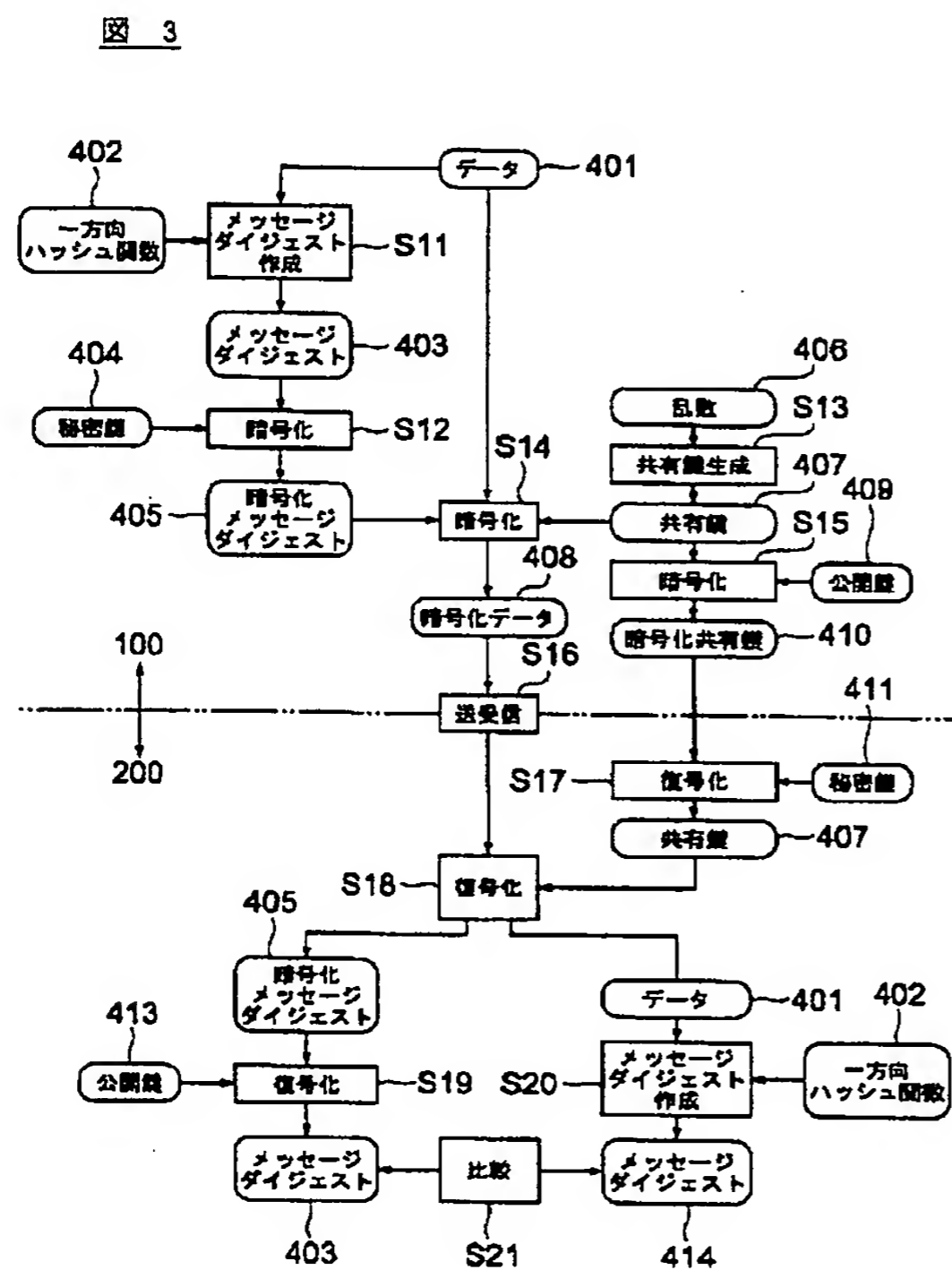
\* 402…MD5 一方向ハッシュ関数  
 403…メッセージダイジェスト  
 404…送信側秘密鍵 (RSA 秘密鍵)  
 405…暗号化メッセージダイジェスト  
 406…乱数  
 407…共有暗号鍵  
 408…暗号化データ  
 409…受信側公開鍵  
 410…暗号化共有鍵  
 10 411…受信側秘密鍵  
 413…送信側公開鍵  
 \* 414…メッセージダイジェスト

【図2】

図 2

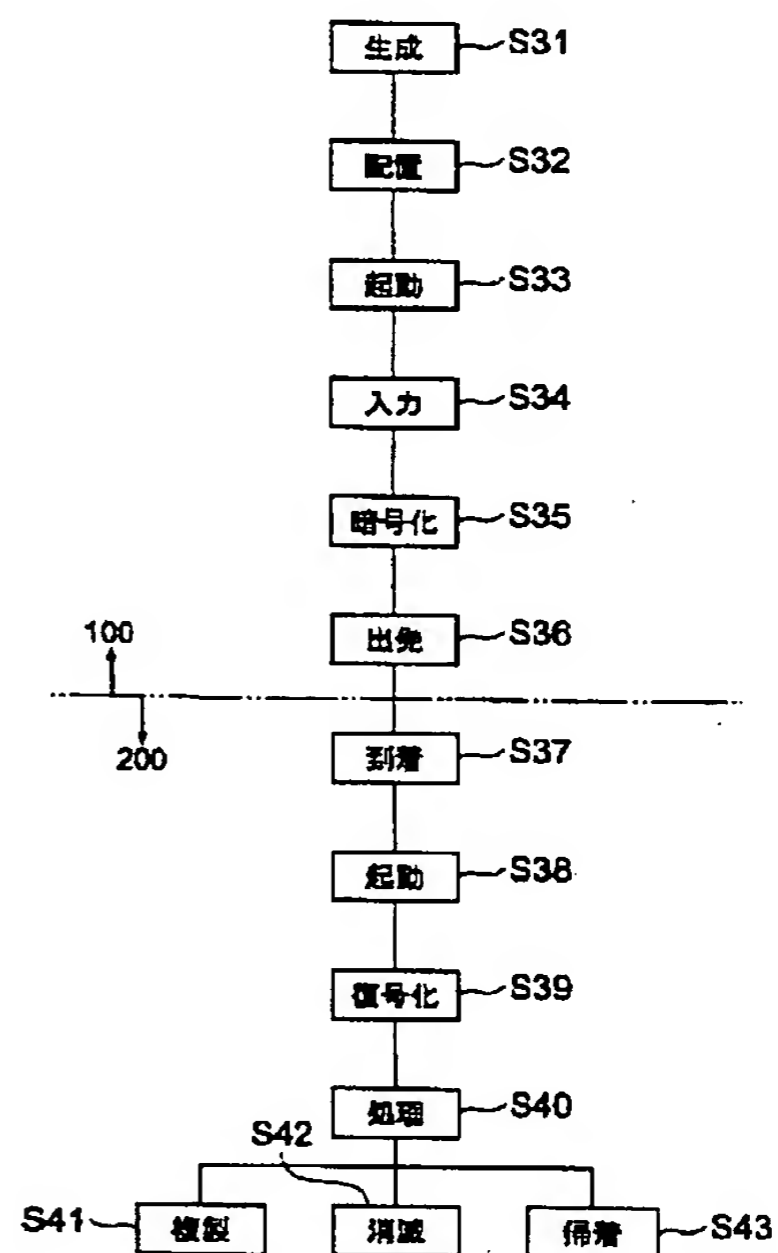


【図3】



【図4】

図4



---

**THIS PAGE BLANK (USPTO)**